AMENDMENTS TO THE CLAIMS:

1. (Currently amended) A storage management system comprising:

a management object for ~~controlling~~ managing a data file in response to a request from a manager ~~which manages a data file to be accessed~~ connected to a network upon an access by a user, said management object ~~certifying~~ authenticating a second manager ID and a second ~~manager~~ password received from the manager, in accordance with a first ID and a first password stored beforehand to authenticate the manager; and

interfaces to be created by said management object when ~~the certification~~ both authentication of the second manager ~~password~~ ID and authentication of the second password by said management object ~~succeeds~~ succeed, and to be expired after a predetermined permission time, said interfaces permitting an access to said data file during said predetermined permission time from the ~~certified~~ authenticated manager.

2. (Original) A storage management system according to claim 1, wherein said interfaces created by said management object are expired by themselves when a log-out sent from the manager at the end of the access is received.

3. (Currently amended) A storage management system according to claim 1, wherein said management object transmits a corresponding cipher key to the manager ~~certified~~ authenticated by the second manager ID and the second password, and the authenticated manager accesses the interfaces by using the cipher key.

4. (Currently amended) A storage management system according to claim 3, wherein said management object ~~create~~ creates different interfaces when ~~the certification~~ authentication of another manager ID and authentication of another password sent from another manager succeeds, to be expired after a predetermined permission time, the ~~difference~~ different interfaces permitting an access to said data file during said predetermined permission time by ~~the certified other~~ said another manager.

5. (Currently amended) A storage management system according to claim 1, wherein said management object ~~has a function of~~ determines not ~~creating~~ to create the interfaces if a non-use period from [[the]] most recent log-out of the manager exceeds a predetermined period when the second manager ID and the second password are ~~certified~~ authenticated.

6. (Currently amended) A storage management system according to claim 1, further comprising an information file for storing a plurality of functions of a remote method invocation protocol each having permission time for a manager and a plurality of flags for defining which manager is permitted to use which function.

7. (Original) A storage management system according to claim 6, wherein said information file stores a flag for temporarily stopping the use of the created interfaces in response to a maintenance request.

8. (Original) A storage management system according to claim 1, further comprising a storage for storing a Java virtual machine having a Java applet program, wherein the Java applet program is transmitted to the manager in response to a request from the manager.

9. (Currently amended) A management program having computer codes readable by a storage management system to run thereon, the program comprising:

a ~~certifying~~ step of ~~certifying~~ authenticating a second manager ID and a second password received from a manager accessing to a data file, in accordance with a first ID and a first password stored beforehand; and

~~an interface creating~~ a step of creating interfaces for the manager if ~~said certifying step succeeds the certification~~ the authenticating of the second manager ~~password~~ ID and the second password ~~succeeds~~ succeeds, said interfaces permitting access by the manager during a predetermined permission time.

10. (Original) A management program according to claim 9, wherein the interfaces are expired by themselves when a log-out sent from the manager at the end of an access is received.

11. (Currently amended) A management program according to claim 9, further comprising a step of transmitting a corresponding cipher key to the manager ~~certified~~ having been authenticated by the second manager ID and the second password.

12. (Currently amended) A management program according to claim 11, further comprising a step of creating different interfaces when the ~~certification~~ authentication of another manager ID and another password sent from another manager succeeds, and to be expired after a predetermined permission time, the ~~difference~~ different interfaces permitting an access to said data file during said predetermined permission time by the ~~certified other~~ another manager.

13. (Currently amended) A management program according to claim 9, ~~wherein there is provided a function~~ further comprising a step of ~~not creating the~~ preventing the creation of interfaces if a non-use period from [[the]] most recent log-out of the manager exceeds a predetermined period when the second manager ID and the second password are ~~certified~~ authenticated.

14. (Original) A management program according to claim 9, wherein there is provided an information file for storing a plurality of functions of a remote method invocation protocol and a plurality of flags for defining which manager is permitted to use which function.

15. (Original) A management program according to claim 14, further comprising a step of storing a flag for temporarily stopping the use of the created interfaces in response to a maintenance request.

16. (Original) A management program according to claim 9, further comprising a step of transmitting a Java applet program from a Java virtual machine to the manager in response to a request from the manager.

17. (Currently amended) A storage management method of ~~controlling~~ managing a request from a manager [[in]] connected through a network to a storage management system ~~controlling~~ managing a data file to be accessed by a user, the method comprising:

~~a certifying step of certifying~~ authenticating a second manager ID and a second ~~manager~~ password received from the manager, in accordance with a first ID and a first password stored beforehand to authenticate the manager; [[and]]

~~a step of~~ creating interfaces when ~~the certification~~ both authentication of the second manager ~~password~~ ID and authentication of the second password ~~succeeds~~ succeed to permit an access by the ~~certified manager, and~~ authenticated manager; and

expiring the interfaces after a lapse of a predetermined permission time.

18. (Currently amended) A storage management method according to claim 17, ~~wherein~~ further comprising expiring the created interfaces ~~are expired~~ by themselves when a log-out sent from the manager at the end of the access is received.

19. (Currently amended) A storage management method according to claim 17, further comprising ~~a step of~~ transmitting a corresponding cipher key to the manager ~~certified~~ having been authenticated by the second manager ID and the second password.

20. (Currently amended) A storage management method according to claim 19, further comprising a step of creating different interfaces when ~~the certification~~ authentication of another manager ID and authentication of another password sent from another manager

succeeds, and to be expired after a predetermined permission time, the ~~difference~~ different interfaces permitting an access to said data file during said predetermined permission time by the ~~certified other~~ another manager.